Krontech

Detection Of Anomaly & User Behavior Analytics

How to detect Anomaly and to use on Security?

Krontech

Sections

01 **General Information**

02 Anomaly Detection Through Keystroke

03 Anomaly Detection Project

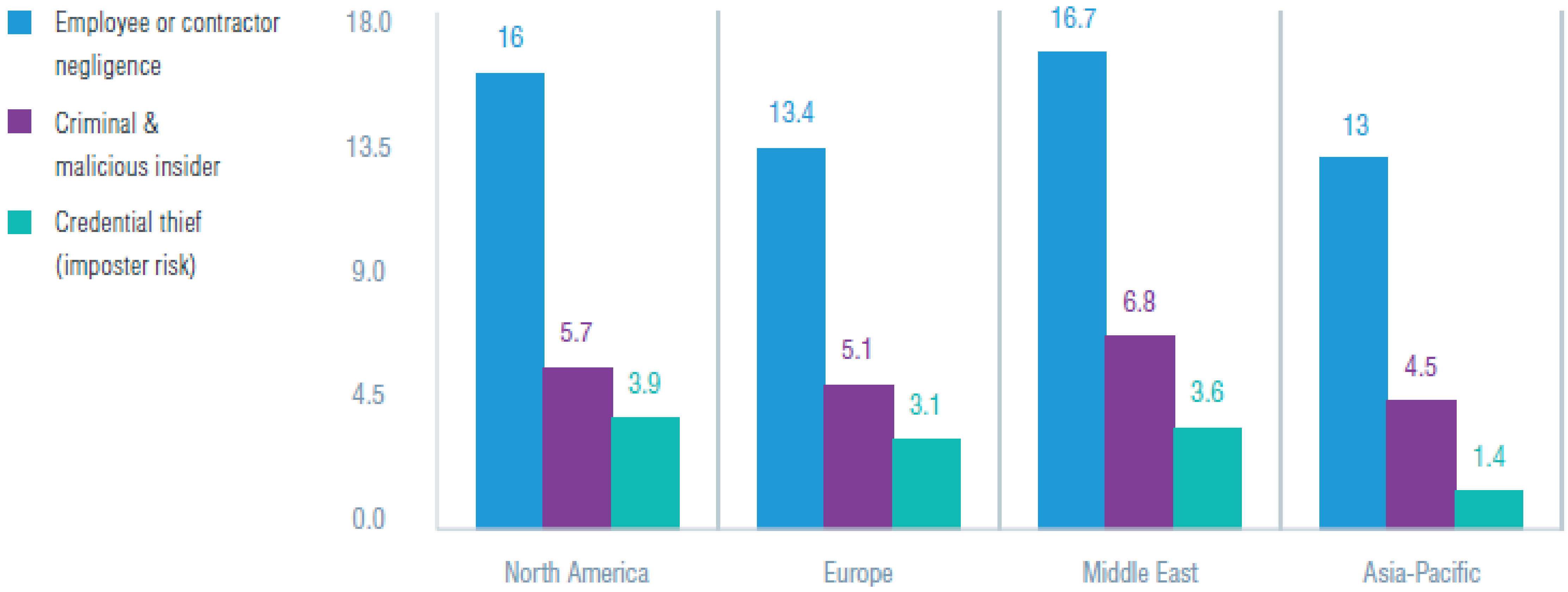
Krontech

General Information

- Today's most damaging security threats do not originate from malicious outsiders or malware but from trusted insiders with access to sensitive data and systems - both malicious insiders and negligent insiders

General Information

Frequency for three profiles of insider incidents by global region



Krontech

General Information

54%

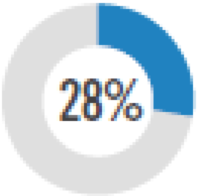
Operational disruption or outage

50%

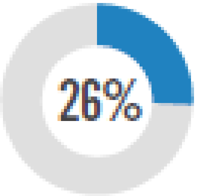
Loss of critical data

38%

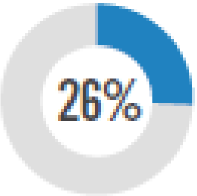
Brand damage



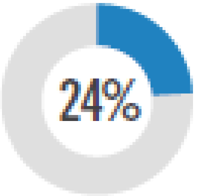
Legal liabilities



Loss in competitive edge



Expenditure remediating successful intrusions



Loss in revenue

Total number of benchmarked organizations

204

Total number of insider incidents

4,716

Total average cost

$11.45M

Incidents relating to negligence

62%

Incidents relating to criminal insider

23%

Incidents relating to user credential theft

14%

Annualized cost for negligence

$4.58M

Annualized cost for criminal insider

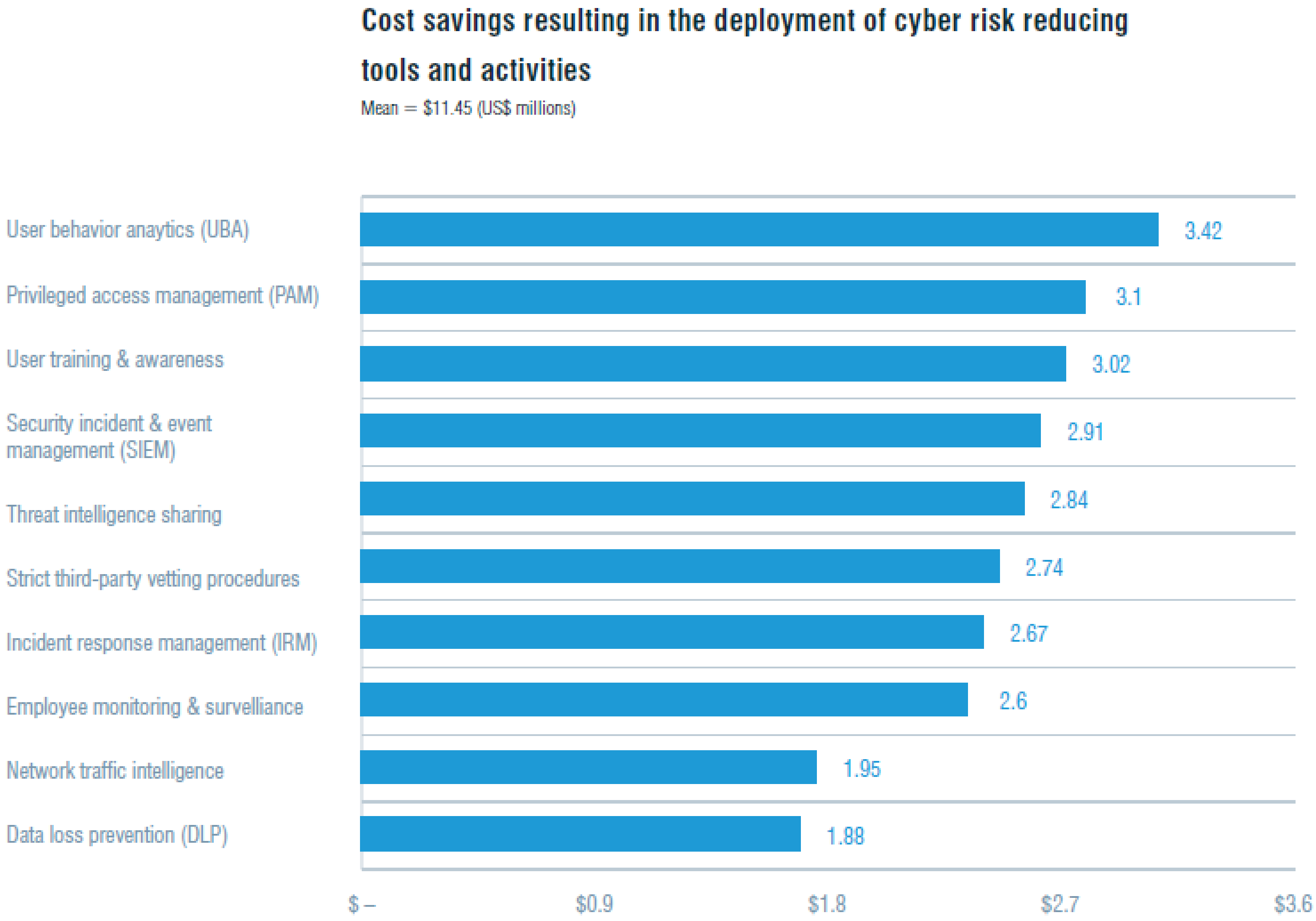
$4.08M

Annualized cost for credential theft

$2.79M

Krontech

General Information



Krontech

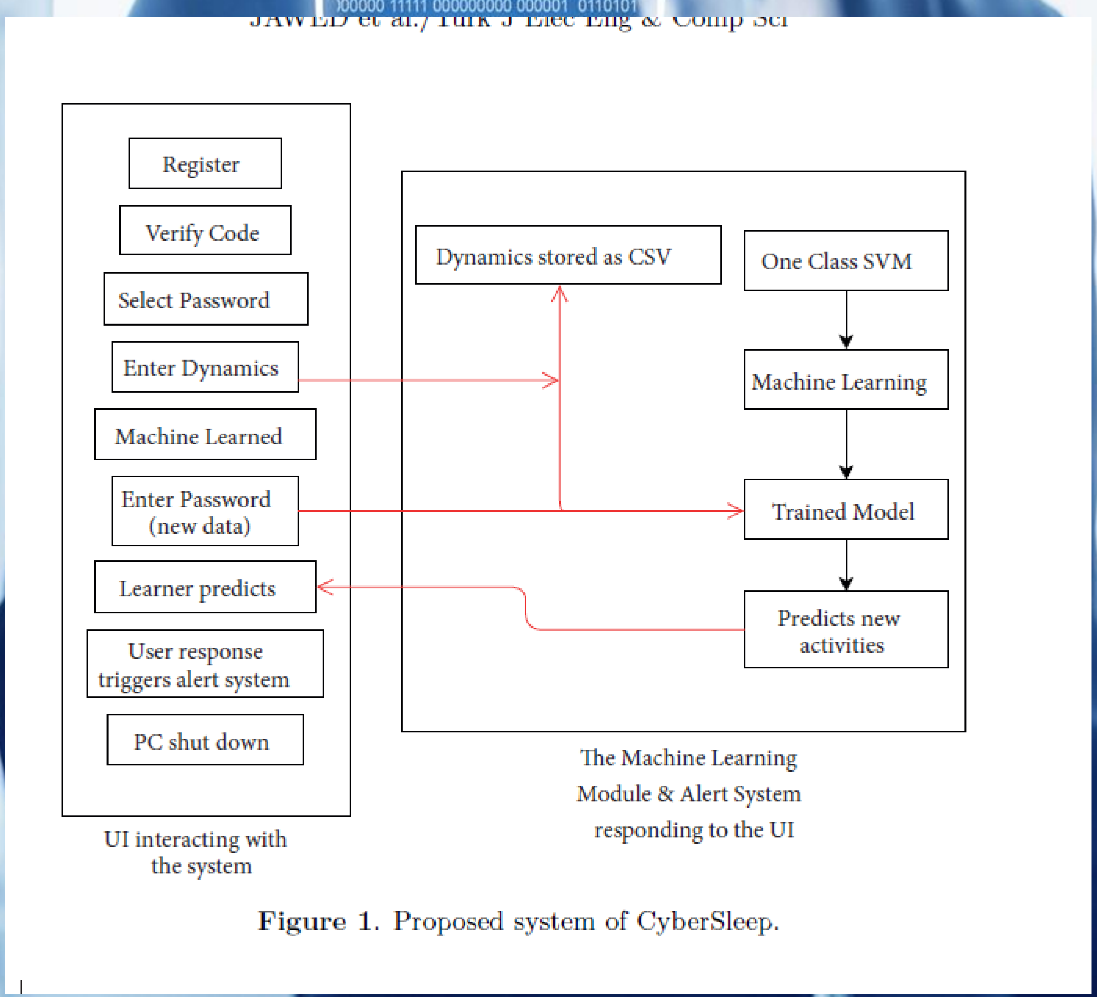
Sections

01 General Information

02 Anomaly Detection Through Keystroke

03 Anomaly Detection Project

Anomaly detection through keystroke and tap dynamics implemented via machine learning algorithms



JAWED et al./Turk J Elec Eng & Comp Sci

Register

Verify Code

Select Password

Enter Dynamics

Machine Learned

Enter Password (new data)

Learner predicts

User response triggers alert system

PC shut down

UI interacting with the system

Dynamics stored as CSV

One Class SVM

Machine Learning

Trained Model

Predicts new activities

The Machine Learning Module & Alert System responding to the UI

Figure 1. Proposed system of CyberSleep.

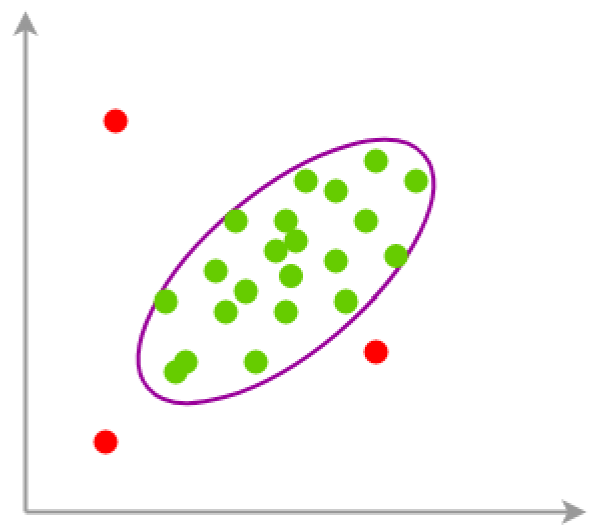
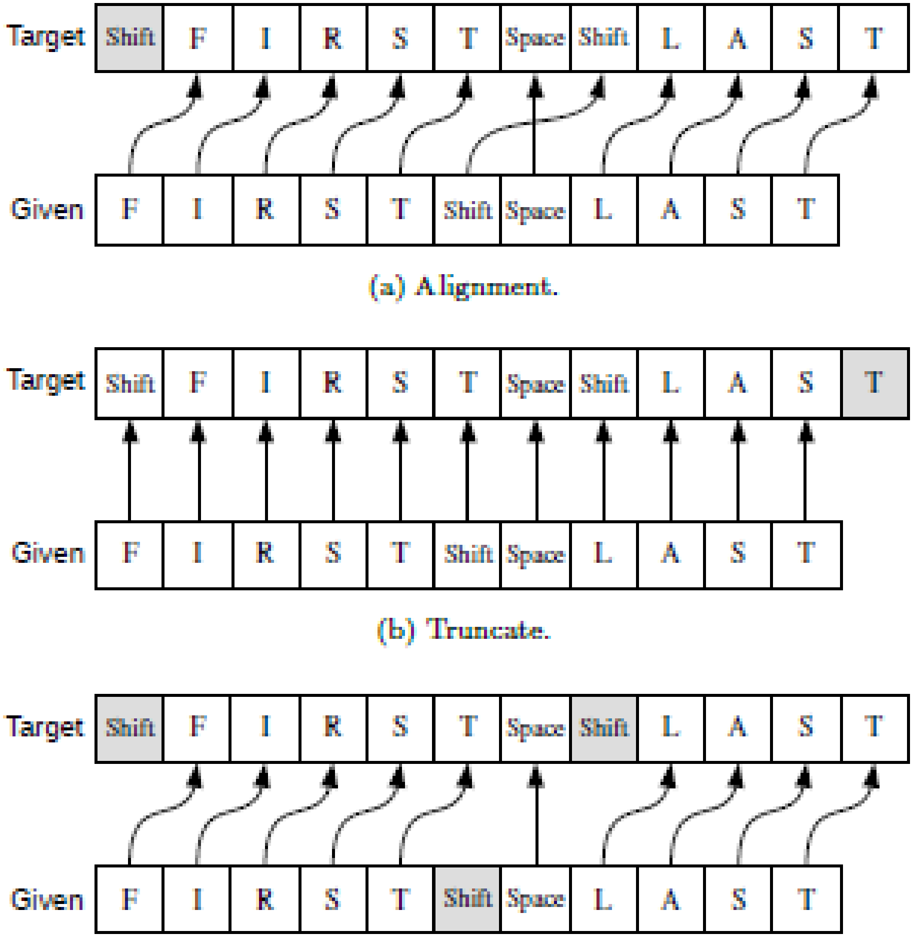


Image copyright: Rukshan Manorathna


Target
Shift F I R S T Space Shift L A S T
Given
F I R S T Shift Space L A S T

(a) Alignment.

Target
Shift F I R S T Space Shift L A S T
Given
F I R S T Shift Space L A S T

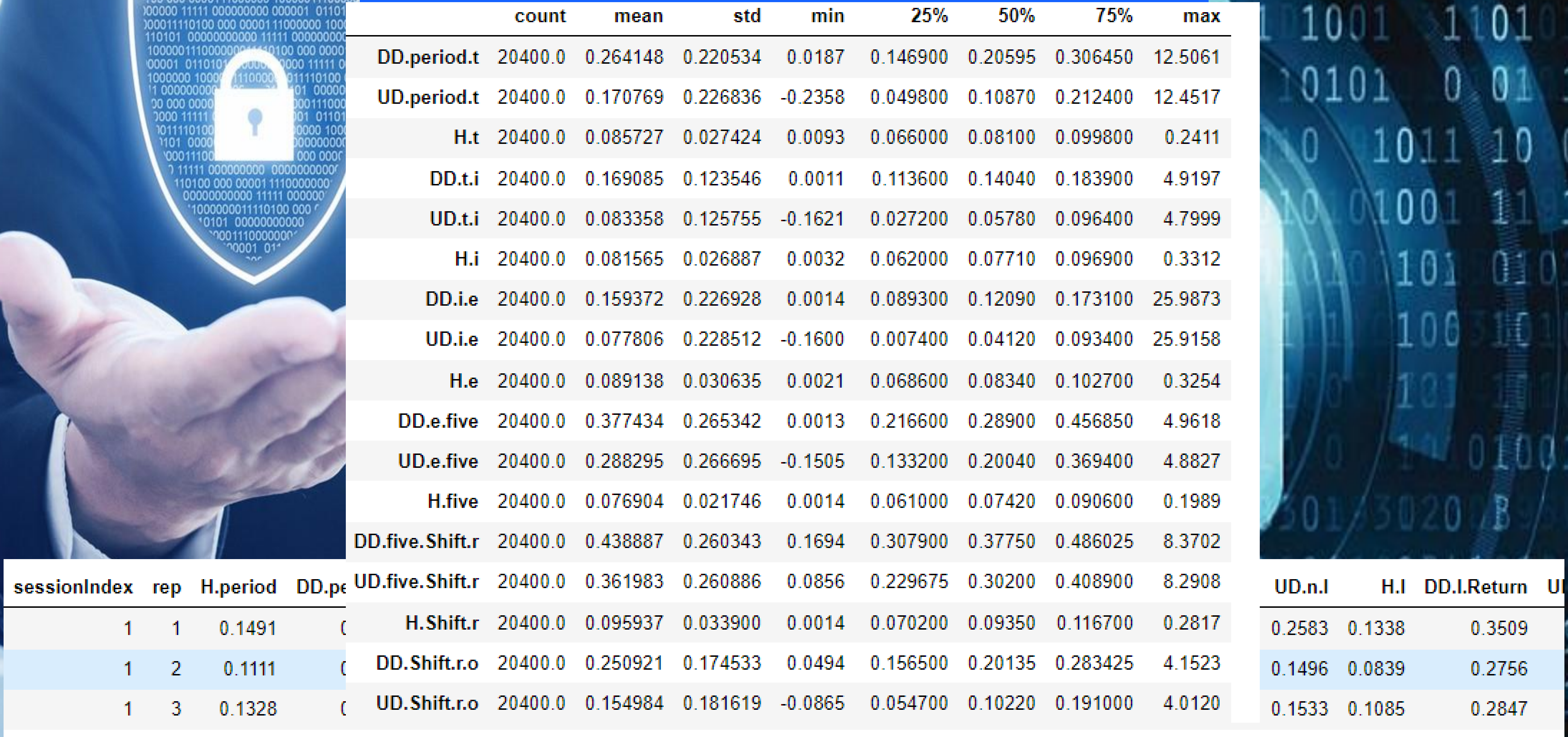
(b) Truncate.

Target
Shift F I R S T Space Shift L A S T
Given
F I R S T Shift Space L A S T

(c) Discard.

Imag

Anomaly detection through keystroke and tap dynamics implemented via machine learning algorithms



	count	mean	std	min	25%	50%	75%	max
DD.period.t	20400.0	0.264148	0.220534	0.0187	0.146900	0.20595	0.306450	12.5061
UD.period.t	20400.0	0.170769	0.226836	-0.2358	0.049800	0.10870	0.212400	12.4517
H.t	20400.0	0.085727	0.027424	0.0093	0.066000	0.08100	0.099800	0.2411
DD.t.i	20400.0	0.169085	0.123546	0.0011	0.113600	0.14040	0.183900	4.9197
UD.t.i	20400.0	0.083358	0.125755	-0.1621	0.027200	0.05780	0.096400	4.7999
H.i	20400.0	0.081565	0.026887	0.0032	0.062000	0.07710	0.096900	0.3312
DD.i.e	20400.0	0.159372	0.226928	0.0014	0.089300	0.12090	0.173100	25.9873
UD.i.e	20400.0	0.077806	0.228512	-0.1600	0.007400	0.04120	0.093400	25.9158
H.e	20400.0	0.089138	0.030635	0.0021	0.068600	0.08340	0.102700	0.3254
DD.e.five	20400.0	0.377434	0.265342	0.0013	0.216600	0.28900	0.456850	4.9618
UD.e.five	20400.0	0.288295	0.266695	-0.1505	0.133200	0.20040	0.369400	4.8827
H.five	20400.0	0.076904	0.021746	0.0014	0.061000	0.07420	0.090600	0.1989
DD.five.Shift.r	20400.0	0.438887	0.260343	0.1694	0.307900	0.37750	0.486025	8.3702
UD.five.Shift.r	20400.0	0.361983	0.260886	0.0856	0.229675	0.30200	0.408900	8.2908
H.Shift.r	20400.0	0.095937	0.033900	0.0014	0.070200	0.09350	0.116700	0.2817
DD.Shift.r.o	20400.0	0.250921	0.174533	0.0494	0.156500	0.20135	0.283425	4.1523
UD.Shift.r.o	20400.0	0.154984	0.181619	-0.0865	0.054700	0.10220	0.191000	4.0120

sessionIndex	rep	H.period	DD.pe	UD.n.l	H.l	DD.l.Return	Ul
1	1	0.1491	(	0.2583	0.1338	0.3509	
1	2	0.1111	(	0.1496	0.0839	0.2756	
1	3	0.1328	(	0.1533	0.1085	0.2847	

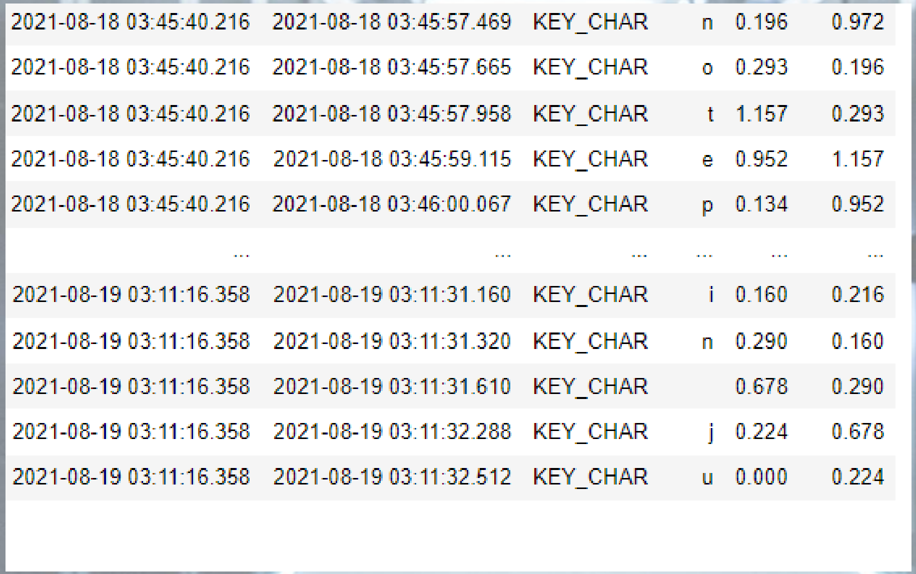
Krontech

Sections

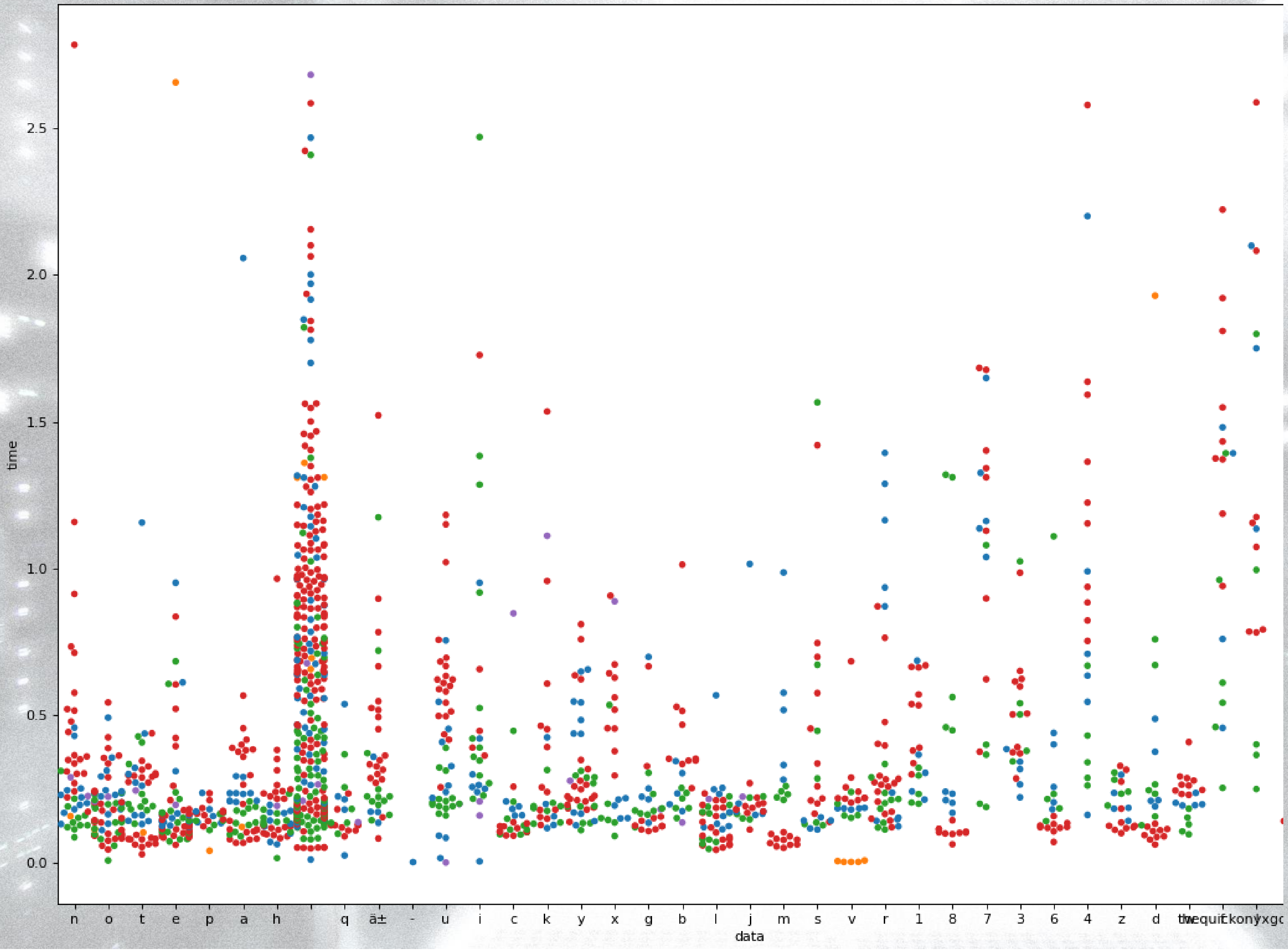
01 General Information

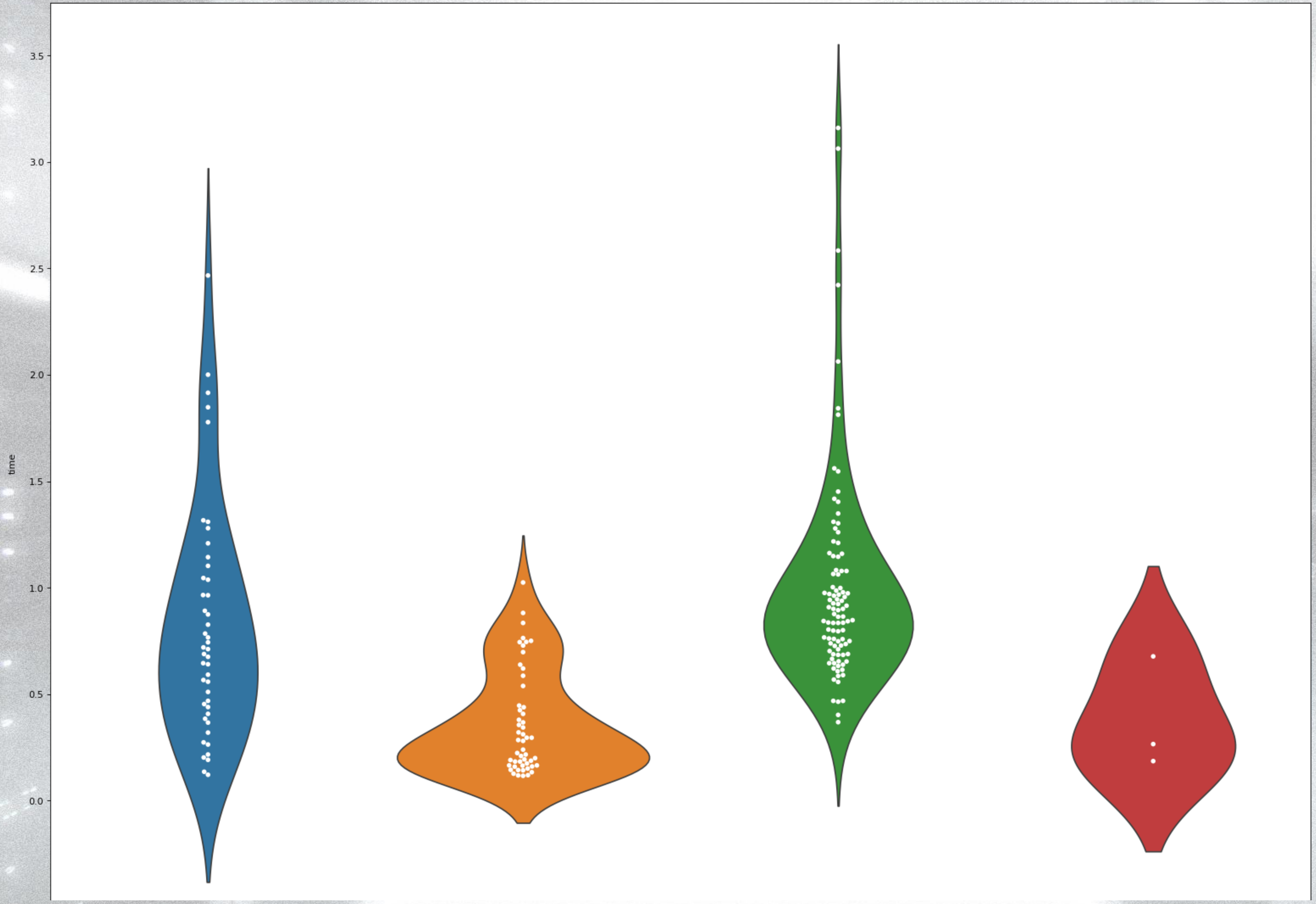
02 Anomaly Detection Through Keystroke

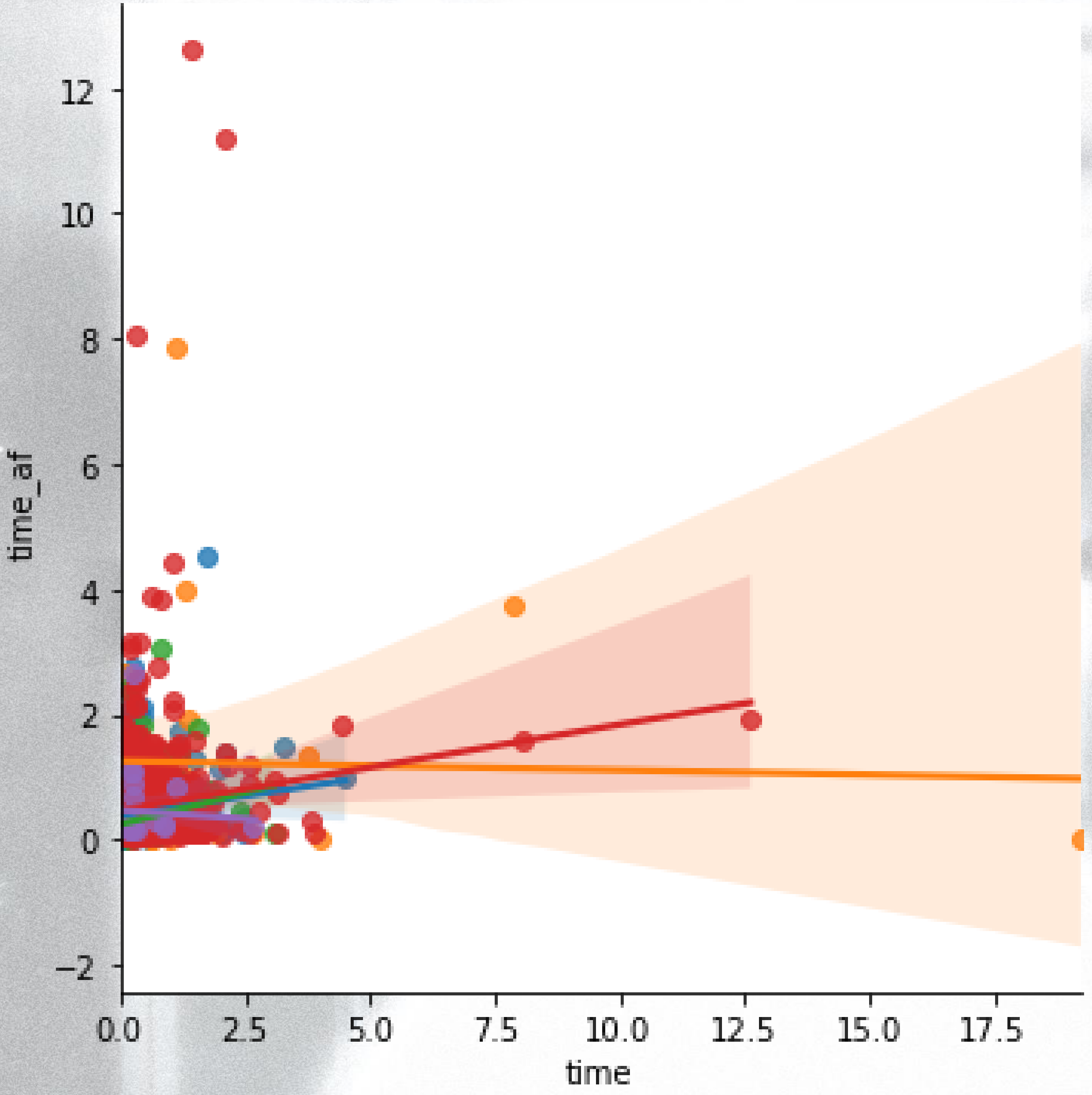
03 Anomaly Detection Project

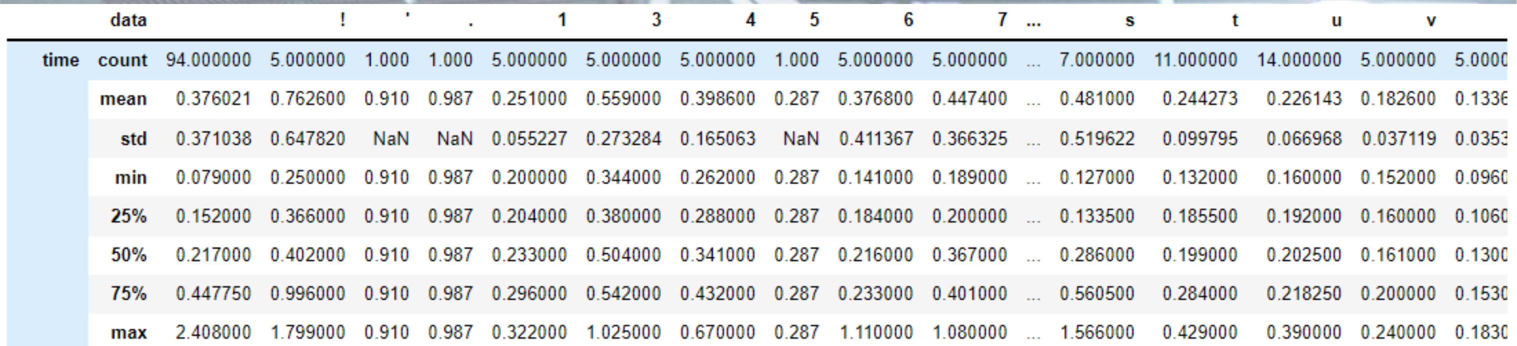


2021-08-18 03:45:40.216	2021-08-18 03:45:57.469	KEY_CHAR	n	0.196	0.972
2021-08-18 03:45:40.216	2021-08-18 03:45:57.665	KEY_CHAR	o	0.293	0.196
2021-08-18 03:45:40.216	2021-08-18 03:45:57.958	KEY_CHAR	t	1.157	0.293
2021-08-18 03:45:40.216	2021-08-18 03:45:59.115	KEY_CHAR	e	0.952	1.157
2021-08-18 03:45:40.216	2021-08-18 03:46:00.067	KEY_CHAR	p	0.134	0.952
...	...	...	...	...	...
2021-08-19 03:11:16.358	2021-08-19 03:11:31.160	KEY_CHAR	i	0.160	0.216
2021-08-19 03:11:16.358	2021-08-19 03:11:31.320	KEY_CHAR	n	0.290	0.160
2021-08-19 03:11:16.358	2021-08-19 03:11:31.610	KEY_CHAR		0.678	0.290
2021-08-19 03:11:16.358	2021-08-19 03:11:32.288	KEY_CHAR	j	0.224	0.678
2021-08-19 03:11:16.358	2021-08-19 03:11:32.512	KEY_CHAR	u	0.000	0.224

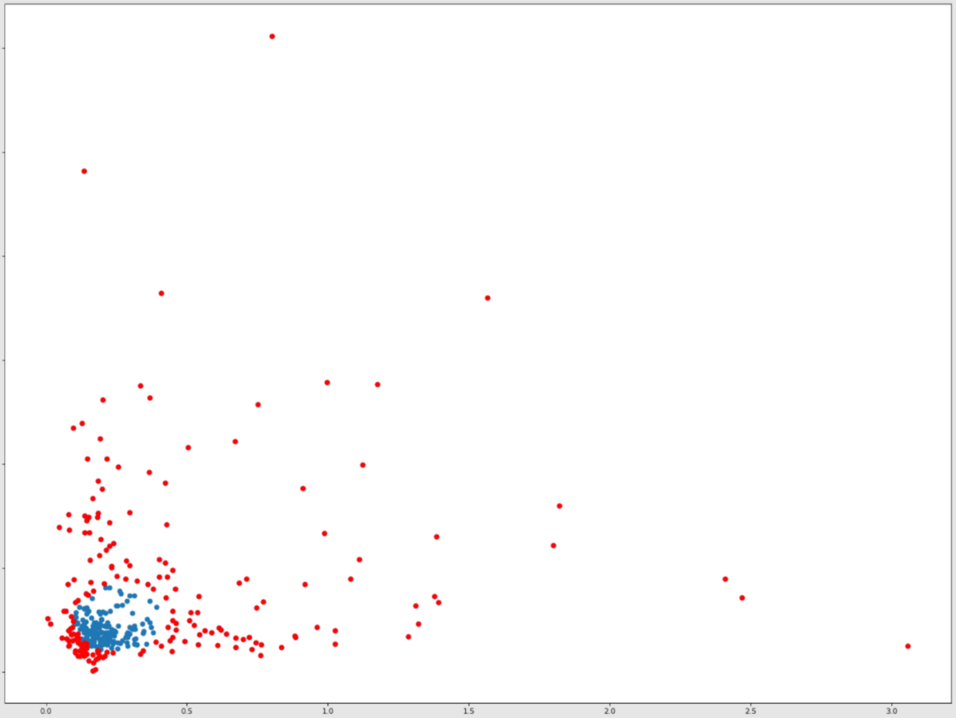

time
0.0
0.5
1.0
1.5
2.0
2.5
data
n
o
t
e
p
a
h
q
ä±
-
u
i
c
k
y
x
g
b
l
j
m
s
v
r
1
8
7
3
6
4
z
d
thequickonyxgo

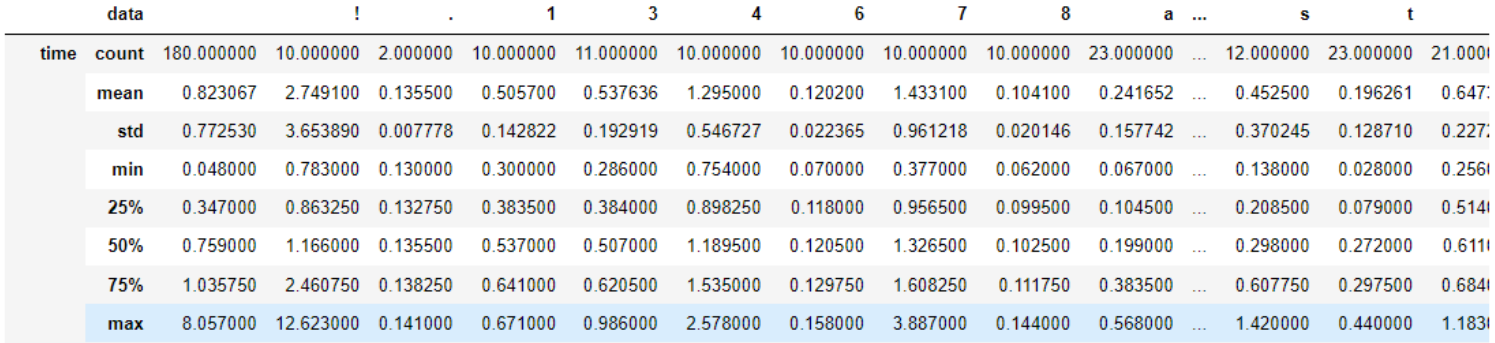

time
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0


time_af
12
10
8
6
4
2
0
−2
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
time

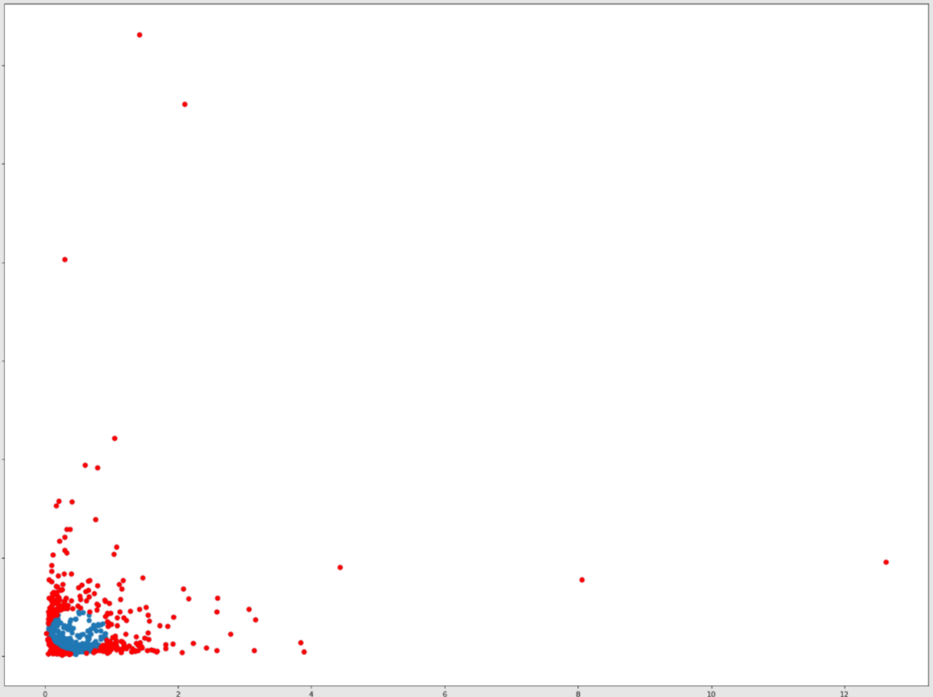


	data		!	'	.	1	3	4	5	6	7	...	s	t	u	v	
time	count	94.000000	5.000000	1.000	1.000	5.000000	5.000000	5.000000	1.000	5.000000	5.000000	...	7.000000	11.000000	14.000000	5.000000	5.0000
	mean	0.376021	0.762600	0.910	0.987	0.251000	0.559000	0.398600	0.287	0.376800	0.447400	...	0.481000	0.244273	0.226143	0.182600	0.1336
	std	0.371038	0.647820	NaN	NaN	0.055227	0.273284	0.165063	NaN	0.411367	0.366325	...	0.519622	0.099795	0.066968	0.037119	0.0353
	min	0.079000	0.250000	0.910	0.987	0.200000	0.344000	0.262000	0.287	0.141000	0.189000	...	0.127000	0.132000	0.160000	0.152000	0.0960
	25%	0.152000	0.366000	0.910	0.987	0.204000	0.380000	0.288000	0.287	0.184000	0.200000	...	0.133500	0.185500	0.192000	0.160000	0.1060
	50%	0.217000	0.402000	0.910	0.987	0.233000	0.504000	0.341000	0.287	0.216000	0.367000	...	0.286000	0.199000	0.202500	0.161000	0.1300
	75%	0.447750	0.996000	0.910	0.987	0.296000	0.542000	0.432000	0.287	0.233000	0.401000	...	0.560500	0.284000	0.218250	0.200000	0.1530
	max	2.408000	1.799000	0.910	0.987	0.322000	1.025000	0.670000	0.287	1.110000	1.080000	...	1.566000	0.429000	0.390000	0.240000	0.1830

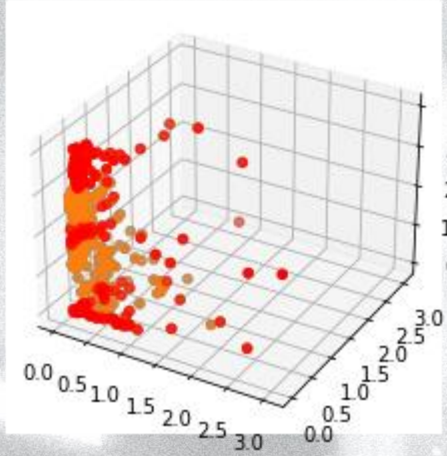


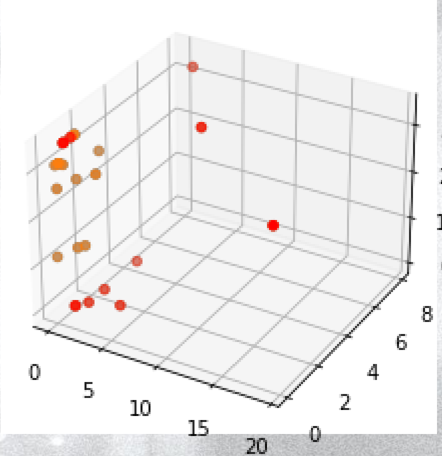


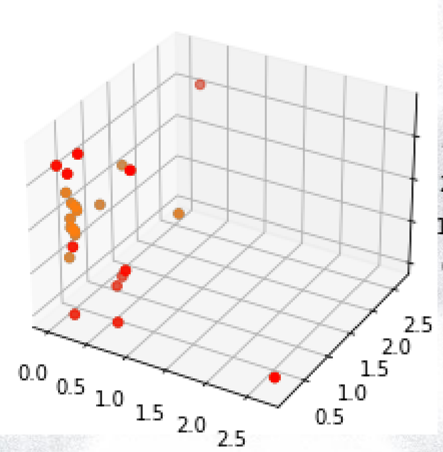
	data		!	.	1	3	4	6	7	8	a	...	s	t	
time	count	180.000000	10.000000	2.000000	10.000000	11.000000	10.000000	10.000000	10.000000	10.000000	23.000000	...	12.000000	23.000000	21.000
	mean	0.823067	2.749100	0.135500	0.505700	0.537636	1.295000	0.120200	1.433100	0.104100	0.241652	...	0.452500	0.196261	0.647
	std	0.772530	3.653890	0.007778	0.142822	0.192919	0.546727	0.022365	0.961218	0.020146	0.157742	...	0.370245	0.128710	0.227
	min	0.048000	0.783000	0.130000	0.300000	0.286000	0.754000	0.070000	0.377000	0.062000	0.067000	...	0.138000	0.028000	0.256
	25%	0.347000	0.863250	0.132750	0.383500	0.384000	0.898250	0.118000	0.956500	0.099500	0.104500	...	0.208500	0.079000	0.514
	50%	0.759000	1.166000	0.135500	0.537000	0.507000	1.189500	0.120500	1.326500	0.102500	0.199000	...	0.298000	0.272000	0.611
	75%	1.035750	2.460750	0.138250	0.641000	0.620500	1.535000	0.129750	1.608250	0.111750	0.383500	...	0.607750	0.297500	0.684
	max	8.057000	12.623000	0.141000	0.671000	0.986000	2.578000	0.158000	3.887000	0.144000	0.568000	...	1.420000	0.440000	1.183

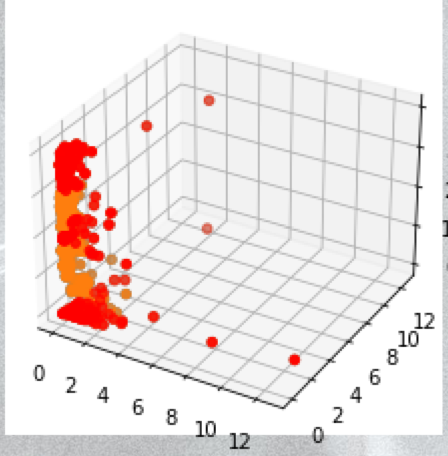


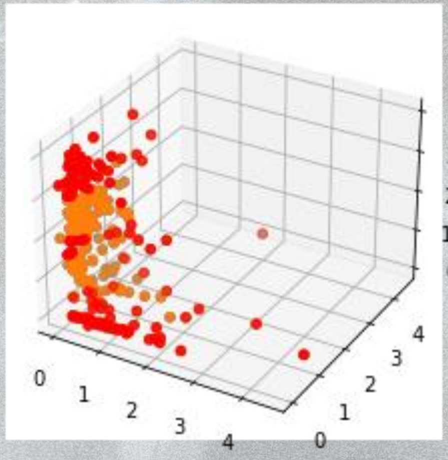
```
{'': 0,
 '!': 1,
 "'": 2,
 '-': 3,
 '.': 4,
 '1': 5,
 '3': 6,
 '4': 7,
 '5': 8,
 '6': 9,
 '7': 10,
 '8': 11,
 'a': 12,
 'b': 13,
 'c': 14,
 'd': 15,
 'e': 16,
 'f': 17,
 'g': 18,
 'h': 19,
 'i': 20,
 'j': 21,
 'k': 22,
 'l': 23,
 'm': 24,
 'n': 25,
 'o': 26,
 'p': 27,
 'q': 28,
 'r': 29,
 's': 30,
 't': 31,
 'thequickon
 'u': 33,
 'v': 34,
 'w': 35,
 'x': 36,
 'y': 37,
 'z': 38,
 'ã§': 39,
 'ä±': 40}
```



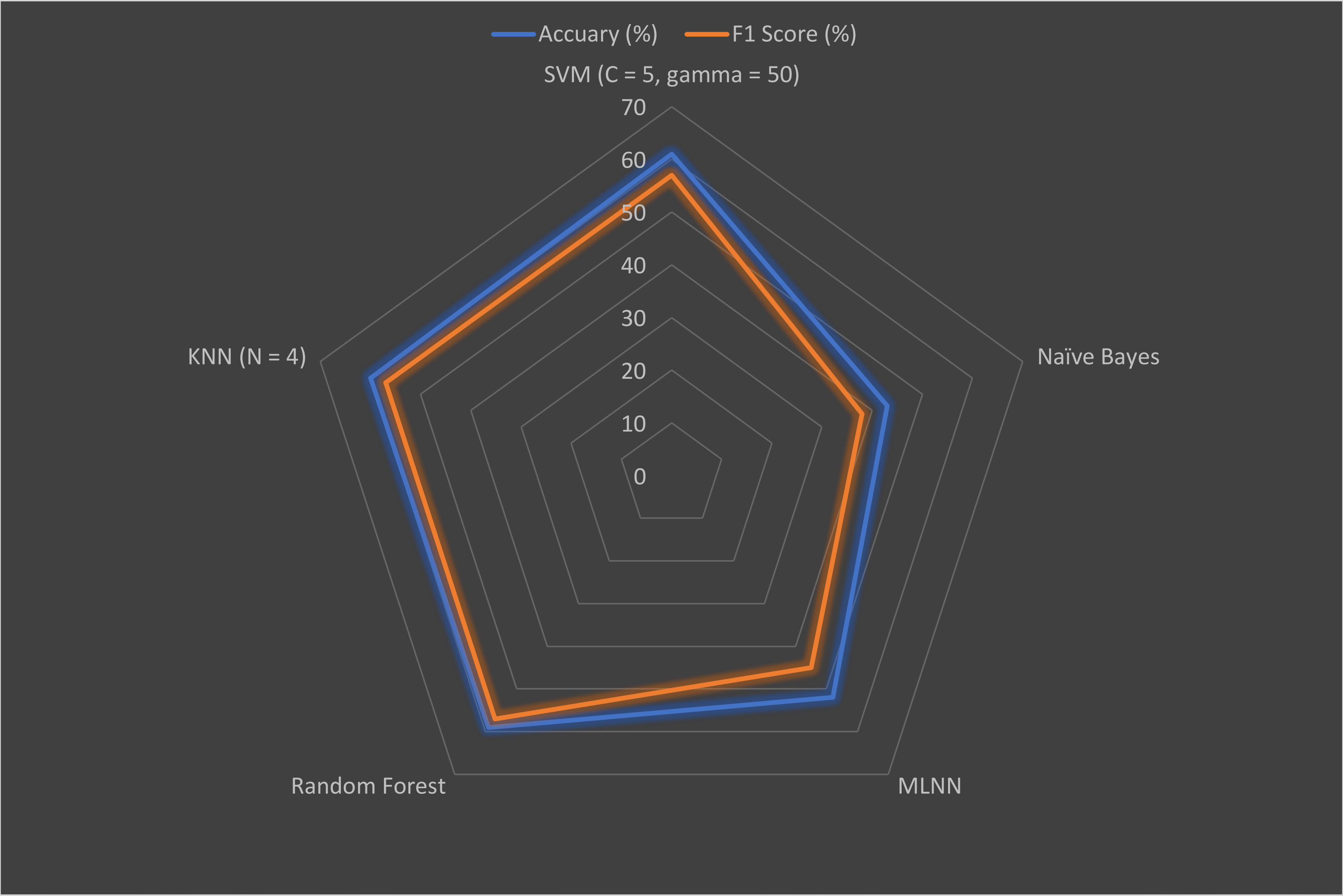








Comparing Anomaly-Detection Algorithms for Keystroke Dynamics



Kron